



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

52

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/782,860	02/14/2001	Frank J. DiSanto	Copy-62	9329

7590

04/15/2005

PLEVY & HOWARD
600 North Easton Road
Willow Grove, PA 19090

EXAMINER

NALVEN, ANDREW L

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 04/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/782,860	Applicant(s) DISANTO ET AL.	
	Examiner Andrew L Nalven	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 27 December 2004.
2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-32 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) 1-32 is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
10) ☒ The drawing(s) filed on 14 February 2001 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>12/27/04</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-32 are pending.
2. IDS submitted 2/14/01 has been received and considered.

Response to Arguments

3. Applicant's arguments filed 12/27/04 have been fully considered but they are not persuasive.
4. Applicant has argued on pages 12-13 that Matsui (US Patent No. 5,488,661) fails to teach "selecting an encryption key from among a plurality of encryption keys dependently upon said extracted data value; and encrypting a subsequent one of said message data blocks using said selected encryption key." Examiner respectfully disagrees. Examiner contends that Matsui teaches the above-cited limitation (Matsui, column 5 line 64 – column 6 line 35 and column 7 lines 13-25). Matsui teaches that a second processing block encrypts a second input data by using a key selected dependently upon the 4 less significant bits of the previous processing block's output (Matsui, column 6 lines 17-35). Hence, Matsui teaches the selection of a key dependently upon a block of data and encrypting a subsequent block using the selected key.

Drawings

Art Unit: 2134

5. This application has been filed with informal drawings which are acceptable for examination purposes only. Formal drawings will be required when the application is allowed.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1-8, 10, 12-19, 21-29, and 31-32 are rejected under 35 U.S.C. 102(b) as being anticipated by Matsui US Patent No. 5,488,661. Matsui discloses a data communication system and method with data scrambling.

8. With regards to claims 1, 13, and 24, Matsui teaches the extracting of a data value from a message data block (Matsui, column 5 line 67 – column 6 line 4, selects less significant 4 bytes), the selecting of an encryption key from among a plurality of encryption keys dependently upon said extracted data value (Matsui, column 6 lines 17-35, extended key), encrypting a subsequent message data block using the selected encryption key (Matsui, column 6 lines 17-35), and transmitting the encrypted data block of the network (Matsui, column 4 lines 15-20, data communication system).

9. With regards to claim 2, Matsui teaches the steps iteratively repeated for each message data block (Matsui, column 6 lines 36-40).

Art Unit: 2134

10. With regards to claims 3,14, and 25, Matsui teaches the receiving of data blocks (Matsui, column 7 lines 28-32, column 5 lines 58-62), decrypting the received data block using a key based on a prior data block (Matsui, column 6 lines 7-13), extracting a data value from a message data block (Matsui, column 5 line 67 – column 6 line 4), and selecting an encryption key from among a plurality of retained encryption keys (Matsui, column 6 lines 4-7).

11. With regards to claims 4 and 15, Matsui teaches the extracted data value is determined using a known number of bits (Matsui, column 5 line 67 – column 6 line 4, 4 bytes).

12. With regards to claims 5, 16, and 26, Matsui teaches the known number of bits being distributed among at least one byte of a data block (Matsui, column 5 line 67 – column 6 line 4).

13. With regards to claims 6,17, and 27, Matsui teaches the known number of bits being located in a first byte of each of said message blocks (Matsui, column 5 line 67 – column 6 line 4, less significant bits).

14. With regards to claims 7, 18 and 28, Matsui teaches the known number of bits being in the last byte of the message blocks (Matsui, column 6 lines 12-16).

15. With regards to claims 8, 19, and 29, Matsui teaches the data block corresponding to at least one unencrypted block (Matsui, column 5 line 67 – column 6 line 4, input plaintext).

16. With regards to claims 10, 22, and 31, Matsui teaches the extracting limiting the extracted value to a known range (Matsui, column 6 lines 55-62, range of 0-3).

Art Unit: 2134

17. With regards to claims 12, 23, and 32, Matsui teaches the known range being substantially comparable to the number of stored encryption keys (Matsui, column 6 lines 55-62, 4 keys, range of 4).
18. With regards to claim 21, Matsui teaches the apparatus operative to select said encryption key based on the extracted data value (Matsui, column 6 lines 4-8 and 55-62).

Claim Rejections - 35 USC § 103

19. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

20. Claims 9, 20, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matsui US Patent No. 5,488,661 in view of McNair US Patent No. 4,642,424.

McNair teaches a cryptographic transmission system.

21. With regards to claims 9, 20, and 30, Matsui, as described above, fails to teach a data block corresponding to a synchronizing indicator. McNair teaches a data block corresponding to a synchronizing indicator (McNair, column 5 lines 5-18). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize McNair's method of synchronizing with Matsui's data scrambling system because it offers the advantage of allowing synchronization to occur between a sender

Art Unit: 2134

and receiver while preventing an attacker from knowing that synchronization thus maintaining a high resistance to cryptanalysis (McNair, column 2 lines 29-48).

22. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Matsui US Patent No. 5,488,661 in view of Neimat et al US Patent No. 5,542,087. Neimat discloses a linear hashing system for distributed records.

23. With regards to claim 11, Matsui, as described above, fails to teach module arithmetic being used to determine a range. Neimat teaches module arithmetic being used to determine a range (Neimat, column 9 lines 23-42, modulus function). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Neimat's method of using modulo arithmetic because it offers the advantage of ensuring that a data range is within an appropriate range of addresses thus ensuring fast memory access (Neimat, column 1 lines 58-66, column 2 lines 18-28, column 4 lines 25-37).

Conclusion

24. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Art Unit: 2134

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.


25. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L Nalven whose telephone number is 571 272 3839 (before October 26, 2004) or 571 272 3839 (after October 26, 2004). The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 571 272 3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Nalven


_____
GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100